



DEPARTMENT OF THE NAVY
NAVAL SUPPLY SYSTEMS COMMAND
5450 CARLISLE PIKE
PO BOX 2050
MECHANICSBURG PA 17055-0791

TELEPHONE NUMBER
COMMERCIAL
AUTOVON
IN REPLY REFER TO:
5230
CIO-8/005

JAN 30 2004

From: Commander, Naval Supply Systems Command

Subj: NAVSUP IMPLEMENTATION OF DOD PUBLIC KEY ENABLING (PKE)
UPDATE

Ref: (a) NAVSUP ltr 5230 CIO-8/018 of 12 Dec 03
(b) CNO Washington DC 221400Z Sep 03
(c) ASD memo of 17 May 01
(d) NAVSUP PKE Implementing Procedures of 19 May 03

Encl: (1) PKE Exemption Criteria
(2) Waiver Form
(3) PKE Status Report

1. This policy letter updates NAVSUP policy guidance of reference (a).

2. The purpose of this policy letter is to emphasize the importance of compliance with the DOD PKE mandate of 1 April 2004. A review of the monthly PKE status required by references (a) and (b) indicates 11 per cent of NAVSUP applications requiring PKE are PKE compliant. Additional effort is required over the next 60 days to ensure that all unclassified "non-public" web servers require DOD PKI user certificates for authentication unless otherwise exempt or have an approved waiver per reference (c). The 1 April 2004 date remains firm for NAVSUP.

3. Enclosure (1) identifies exemption criteria. Enclosure (2) is a Waiver Form. PKE remains an integral part of system accreditation where required. NAVSUP System accreditation documentation shall address PKE.

4. NAVSUP PKE Implementing Procedures and technical guidance were provided in reference (d) and remain unchanged. NAVSUP strategy is to PKE applications in the most cost effective means available, consistent with application requirements and least impact on users. Responsibility for PKE remains with the Program Manager.

5. Commanding Officers shall ensure activity Program Managers, ISSOs and ISSMs review and validate the enclosure (3) listing of applications/systems. Additionally, the remarks column shall include date system or application will be PKE compliant or a waiver shall be provided. Monthly PKE status reports are due to Mr. Rich Luckenbill prior to the 28th of each month for consolidation and reporting to CNO.

Subj: NAVSUP IMPLEMENTATION OF DOD PUBLIC KEY ENABLING (PKE)
UPDATE

6. All Program Managers without a PKE plan or waiver submission will be required to provide monthly status in CIO meetings beginning March 2004. The NAVSUP points of contact are Ms. Pamela Wenner, NAVSUP IA Program manager at 717-605-7535 (DSN 430) and Mr. Richard Luckenbill at 717-605-7676 (DSN 430).



RUTH L. SANDERS
Command Information Officer

Distribution:
FISC Jacksonville
FISC Norfolk
FISC Pearl Harbor
FISC Puget Sound
FISC San Diego
FISC Yokosuka
NAVICP
NAVSISA
NOLSC
NEXCOM

SYSTEM EXEMPTION CRITERIA FOR PKE

1. Systems or applications that are public web sites.
2. Legacy web-based systems/applications scheduled for phase-out or replacement by April 2004.
3. Systems or applications whose user community includes individuals not programmed to receive DOD PKI certificates (retirees, dependents, and academia).
4. Applications that limit access only for preserving copy write protection of contained information.
5. Development and/or testing web servers.
6. Web sites that limit access only to links, where sites are themselves restricted via PKI certificates.
7. Systems or applications not web based (PKE not required until 2007).

**PUBLIC KEY ENABLING COMPLIANCE WAIVER
REQUEST FORMAT**

All waiver requests must be submitted in writing and signed by the application Program Manager.

1. Request Contact Information
 - a. Waiver Requestor
 - i. Phone Number
 - ii. Email Address
 - iii. Mailing Address
 - b. Application Manager (individual with primary responsibility for operation and oversight of the application - if different from Waiver Requestor above:
 - i. Phone Number
 - ii. Email Address
 - iii. Mailing Address
 - c. Application DAA (Designated Approval Authority):
 - i. Phone Number
 - ii. Email Address
 - iii. Mailing Address
2. Application Information
 - a. Application Name
 - b. IT Registry Database Number (if unknown, leave blank)
 - c. Mission Category
 - d. Purpose (brief functional description)
 - e. Type (Web-based, email, legacy, financial, personnel, supply, etc.)
 - f. Certification (DITSCAP, JITC interoperability, NIAP, etc.)
3. Justification for Waiver
 - a. Identify specific Waiver Criteria for which Request is being made (near term replacement of legacy system, anticipated cost of PK enabling, or undue hardship) see reference (d) of NAVSUP PKE Implementing Procedures.
 - b. Explain/justify basis for selected criteria and identify waiver time required.

The authority for waiver approval rests with the DOD and the DONCIO. Waivers shall be granted only for the minimum length of time required to achieve compliance. In cases where all system users cannot reasonably obtain a PKI certificate by 1 April 2004, applications should allow users continued access via userid and password until a certificate is available. If this option is not feasible, a waiver may be submitted to bridge the gap until situation is resolved.